



Computer and Information Sciences

Complex Systems

Improving the Foundations of Complex System Modeling and Design

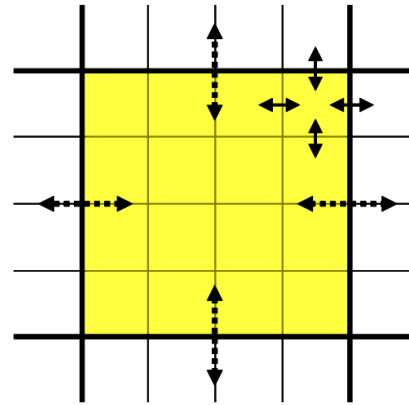
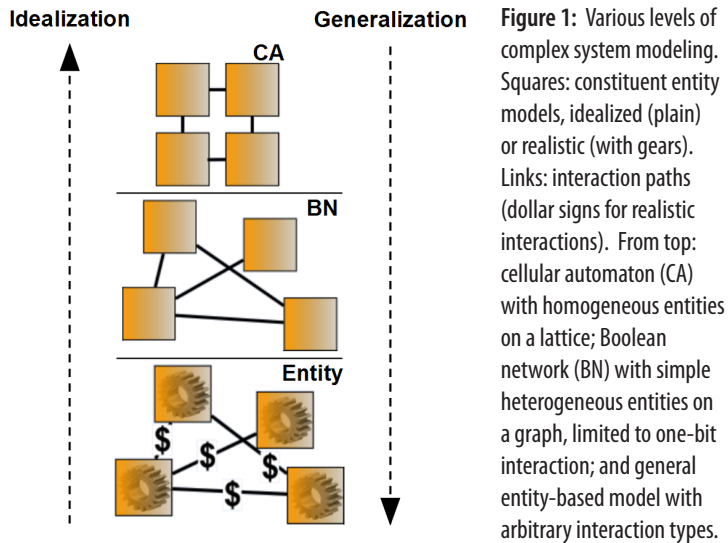


Figure 2: Schematic of renormalization in the case of lattice interactions. Initial entities interact with neighbors (solid arrows) on a fine lattice (light gridlines). A higher-level entity (entire yellow square) interacts with neighbors (dashed arrows) on a coarsened lattice (heavy gridlines), with the new interactions designed to preserve the system's large-scale behavior.

Complexity science has possible applications in cybersecurity

For more information:

Technical Contacts:

Jackson R. Mayo
925-294-6766
jmayo@sandia.gov

Robert C. Armstrong
925-294-2470
rob@dancer.ca.sandia.gov

Science Matters Contact:

Alan Burns
505-844-9642
aburns@sandia.gov

Many complex systems that impact national security, such as energy infrastructure, terrorist networks, and the internet, differ from systems traditionally investigated in science and engineering by exhibiting intricate interactions among large numbers of entities that collectively display unpredictable emergent behavior. Emergent behaviors of complex systems, including self-organization and robustness, can be captured via simulation of interacting subsystems, an approach known as entity-based modeling. Absent conservation laws or an equation of motion, however, the construction of entity-based models is often *ad-hoc* and heuristic, more craft than science. Furthermore, the optimization of real-world simulations to achieve a desired behavior, such as making computers more secure or destabilizing a terrorist network, is often a matter of trial and error. The developing field of complexity science offers a new paradigm for modeling and design to complement traditional approaches. Through systematic studies relating models and emergent

behavior at various levels of abstraction, Sandia's work in complexity science can guide the construction of entity-based models achieving a known or desired emergent behavior.

Complex systems evolve through networked interactions of their constituent entities and often exhibit emergent global behaviors that are not readily predictable from entity properties. To understand these behaviors, research at Sandia (in collaboration with MIT) has made use of idealized models such as cellular automata and Boolean networks. Insights obtained in these settings can be extended to more general entity-based models (Figure 1). Idealized computational studies have validated methods such as renormalization, a technique adapted from theoretical physics for constructing approximate coarse-grained models (Figure 2). Renormalization of complex system models provides a precise framework for understanding the abstraction process (the representation of lower-level entities by higher-level entities) that underlies

practical simulations. The ability of renormalization to preserve certain emergent behaviors (Figure 3) suggests applications to more realistic complex systems.

Cybersecurity, the struggle to mitigate malicious intrusion into computer systems, is a national security challenge with a particular need for insights from complexity science. Due to the scale and sophistication of modern computer software along with classic mathematical results on undecidability, traditional engineering approaches have failed to curb the vulnerabilities of computer systems. Indeed, the practical impossibility of ensuring software correctness has given hackers an asymmetric advantage and led to a proliferation of malicious software exploiting the vulnerabilities (Figure 4).

Potential cybersecurity solutions drawing on complexity science are aimed at reversing this asymmetry. The interaction networks (physical or virtual) in a computer system can be studied in terms of coarse-grained models and emergent behavior; system characteristics that lead to global robustness can guide software design. Furthermore, compelling analogies exist to the naturally occurring complex systems of biology (as indicated by terminology such as computer viruses); genetics, evolution, and ecology can provide theoretical insights and practical strategies for mitigating threats. As Sandia tackles emerging mission areas, complexity science shows encouraging prospects for advancing cybersecurity and other national priorities.

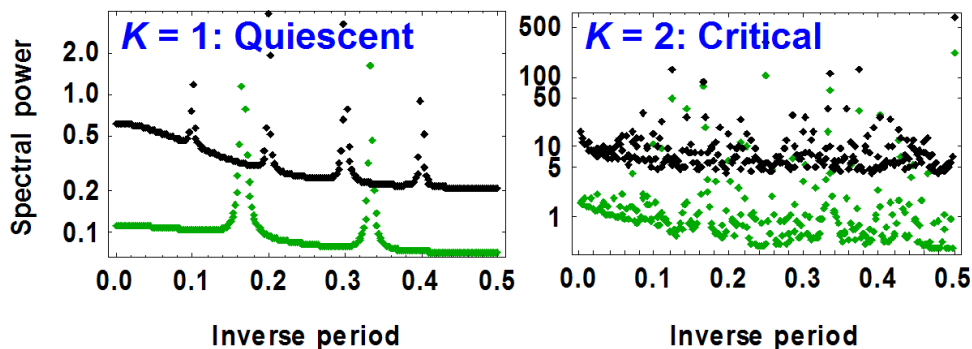


Figure 3: Comparison of emergent behavior of Boolean networks under renormalization. The initial Boolean networks are parameterized by K , the number of in-bound links to each node (entity). Plots show frequency spectrum of simulated dynamics for a 500-node initial graph (black points) and its 100-node coarsening (green points). The qualitative features distinguishing the “quiescent” and “critical” regimes are preserved.

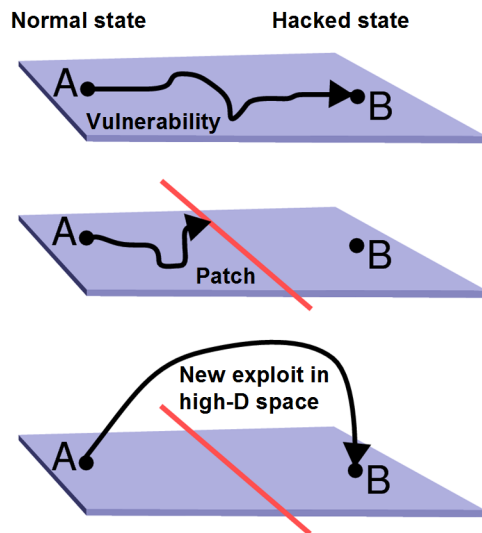


Figure 4: Origin of asymmetric threats to cybersecurity. A computer’s vast state space defies complete verification; a vulnerability is quickly found and exploited (top). An analysis leading to a software patch (middle) can consider only a small subspace of states (violet slab). Other exploits act outside this subspace (bottom), thus turning current cyber defenses into “Majinot lines.”